Министерство науки и высшего образования РФ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
АМУРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
(ФГБОУ ВО «АмГУ»)

Введение в профессию, включая информационно-библиографическую культуру
сборник учебно-методических материалов

для направления подготовки 10.03.01 «Информационная безопасность»

Благовещенск, 2019

Печатается по решению
редакционно-издательского совета
факультета математики и информатики
Амурского государственного
университета

Составитель: Акилова И.М.

Дискретная математика: сборник учебно-методических материалов для направления подготовки для направления подготовки 10.03.01 «Информационная безопасность». – Благовещенск: Амурский гос. ун-т, 2019.

КРАТКОЕ ИЗЛОЖЕНИЕ ЛЕКЦИОННОГО МАТЕРИАЛА

ВВЕДЕНИЕ В ИНФОРМАЦИОННУЮ БЕЗОПАСНОСТЬ

Компьютеры: преступления, признаки уязвимости и меры защиты

Информационная Эра привела к драматическим изменениям в способе выполнения своих обязанностей для большого числа профессий. Теперь нетехнический специалист среднего уровня может выполнять работу, которую раньше делал высококвалифицированный программист. Служащий имеет в своем распоряжении столько точной и оперативной информации, сколько никогда не имел.

Но использование компьютеров и автоматизированных технологий приводит к появлению ряда проблем для руководства организацией. Компьютеры, часто объединенные в сети, могут предоставлять доступ к колоссальному количеству самых разнообразных данных. Поэтому люди беспокоятся о безопасности информации и наличии рисков, связанных с автоматизацией и предоставлением гораздо большего доступа к конфиденциальным, персональным или другим критическим данным. Все увеличивается число компьютерных преступлений, что может привести в конечном счете к подрыву экономики. И поэтому должно быть ясно, что информация - это ресурс, который надо защищать.

Ответственность за защиту информации лежит на низшем звене руководства. Но также кто-то должен осуществлять общее руководство этой деятельностью, поэтому в организации должно иметься лицо в верхнем звене руководства, отвечающее за поддержание работоспособности информационных систем.

И так как автоматизация привела к тому, что теперь операции с вычислительной техникой выполняются простыми служащими организации, а не специально подготовленным техническим персоналом, нужно, чтобы конечные пользователи знали о своей ответственности за защиту информации.

Целью этого документа является дать основы компьютерной безопасности для низшего звена управления, то есть для начальников отделов, руководителей групп и т.п.

При ограблении банка потери в среднем составляют 19 тысяч долларов, а при компьютерном преступлении - 560 тысяч долларов

Число компьютерных преступлений растет - также увеличиваются масштабы компьютерных злоупотреблений. По оценке специалистов США, ущерб от компьютерных преступлений увеличивается на 35 процентов в год и составляет около 3.5 миллиардов долларов. Одной из причин является сумма денег, получаемая в результате преступления: в то время как ущерб от среднего компьютерного преступления составляет 560 тысяч долларов, при ограблении банка - всего лишь 19 тысяч долларов.

Шансов быть пойманным у компьютерного преступника гораздо меньше, чем у грабителя банка - и даже при поимке у него меньше шансов попасть в тюрьму. Обнаруживается в среднем 1 процент компьютерных преступлений. И вероятность того, что за компьютерное мошенничество преступник попадет в тюрьму, меньше 10 процентов.

Умышленные компьютерные преступления составляют заметную часть преступлений. Но злоупотреблений компьютерами и ошибок еще больше. Как выразился один эксперт, "мы теряем из-за ошибок больше денег, чем могли бы украсть". Эти потери подчеркивают важность и серьезность убытков, связанных с компьютерами.

Основной причиной наличия потерь, связанных с компьютерами, является недостаточная образованность в области безопасности. Только наличие некоторых знаний в области безопасности может прекратить инциденты и ошибки, обеспечить эффективное применение мер защиты, предотвратить преступление или своевременно обнаружить подозреваемого. Осведомленность конечного пользователя о мерах безопасности обеспечивает четыре уровня защиты компьютерных и информационных ресурсов:

Меры защиты: четыре уровня защиты

Предотвращение - только авторизованный персонал имеет доступ к информации и технологии

Обнаружение - обеспечивается раннее обнаружение преступлений и злоупотреблений, даже если механизмы защиты были обойдены

Ограничение - уменьшается размер потерь, если преступление все-таки произошло несмотря на меры по его предотвращению и обнаружению

Восстановление - обеспечивается эффективное восстановление информации при наличии документированных и проверенных планов по восстановлению

Вчера контроль за технологией работы был заботой технических администраторов. Сегодня контроль за информацией стал обязанностью каждого нетехнического конечного пользователя. Контроль за информацией требует новых знаний и навыков для группы нетехнических служащих. Хороший контроль за информацией требует понимания возможностей совершения компьютерных преступлений и злоупотреблений, чтобы можно было в дальнейшем предпринять контрмеры против них.

Когда компьютеры впервые появились, они были доступны только небольшому числу людей, которые умели их использовать. Обычно они помещались в специальных помещениях, удаленных территориально от помещений, где работали служащие. Сегодня все изменилось. Компьютерные терминалы и настольные компьютеры используются везде. Компьютерное оборудование стало дружественным к пользователю, поэтому много людей могут быстро и легко научиться тому, как его использовать.

Число служащих в организации, имеющих доступ к компьютерному оборудованию и информационной технологии, постоянно растет. Доступ к информации больше не ограничивается только узким кругом лиц из верхнего руководства организации. Этот процесс привел к тому, что произошла "демократизация преступления". Чем больше людей получало доступ к информационной технологии и компьютерному оборудованию, тем больше возникало возможностей для совершения компьютерных преступлений.

Трудно обобщать, но теперь компьютерным преступником может быть .

· конечный пользователь, не технический служащий и не хакер
· тот, кто не находится на руководящей должности
· тот, у кого нет судимостей
· умный, талантливый сотрудник
· тот, кто много работает
· тот, кто не разбирается в компьютерах
· тот, кого вы подозревали бы в последнюю очередь
· именно тот, кого вы взяли бы на работу

Компьютерным преступником может быть любой

Типичный компьютерный преступник - это не молодой хакер, использующий телефон и домашний компьютер для получения доступа к большим компьютерам. Типичный компьютерный преступник - это служащий, которому разрешен доступ к системе, нетехническим пользователем которой он является. В США компьютерные преступления, совершенные служащими, составляют 70-80 процентов ежегодного ущерба, связанного с компьютерами. Остальные 20 процентов дают действия нечестных и недовольных сотрудников. И совершаются они по целому ряду причин.

Почему люди совершают компьютерные преступления

· личная или финансовая выгода
· развлечение
· месть
· попытка добиться расположения кого-либо к себе
· самовыражение
· случайность
· вандализм

Но значительно больший ущерб, около 60 процентов всех потерь, наносят ошибки людей и инциденты. Предотвращение компьютерных потерь, как из-за умышленных преступлений, так и из-за неумышленных ошибок, требует знаний в области безопасности. Опросы, проводимые периодически в США, показывают, что именно служащие, имевшие знания в области компьютерной безопасности, были основной причиной выявления компьютерных преступлений.

Признаки компьютерных преступлений

Обращайте внимание на:

· неавторизованное использование компьютерного времени
· неавторизованные попытки доступа к файлам данных
· кражи частей компьютеров
· кражи программ
· физическое разрушение оборудования
· уничтожение данных или программ
· неавторизованное владение дискетами, лентами или распечатками

И это только самые очевидные признаки, на которые следует обратить внимание при выявлении компьютерных преступлений. Иногда эти признаки говорят о том, что преступление уже совершено, или что не выполняются меры защиты. Они также могут свидетельствовать о наличии уязвимых мест - указать, где находится дыра в защите - и помочь наметить план действий по устранению уязвимого места. В то время как признаки могут помочь выявить преступление или злоупотребление - меры защиты могут помочь предотвратить его.

Меры защиты - это меры, вводимые руководством, для обеспечения безопасности информации - административные руководящие документы(приказы, положения, инструкции), аппаратные устройства или дополнительные программы - основной целью которых является предотвратить преступления и злоупотребления, не позволив им произойти. Меры защиты могут также выполнять функцию ограничения, уменьшая размер ущерба от преступления.

Информационная безопасность

То, что в 60-е годы называлось компьютерной безопасностью, а в 70-е - безопасностью данных, сейчас более правильно именуется информационной безопасностью. Информационная безопасность подчеркивает важность информации в современном обществе - понимание того, что информация - это ценный ресурс, нечто большее, чем отдельные элементы данных.

Информационной безопасностью называют меры по защите информации от неавторизованного доступа, разрушения, модификации, раскрытия и задержек в доступе. Информационная безопасность включает в себя меры по защите процессов создания данных, их ввода, обработки и вывода. Целью информационной безопасности является обезопасить ценности системы, защитить и гарантировать точность и целостность информации, и минимизировать разрушения, которые могут иметь место, если информация будет модифицирована или разрушена. Информационная безопасность требует учета всех событий, в ходе которых информация создается, модифицируется, к ней обеспечивается доступ или она распространяется.

Информационная безопасность дает гарантию того, что достигаются следующие цели:

· конфиденциальность критической информации
· целостность информации и связанных с ней процессов (создания, ввода, обработки и вывода)
· доступность информации, когда она нужна
· учет всех процессов, связанных с информацией

Некоторые технологии по защите системы и обеспечению учета всех событий могут быть встроены в сам компьютер. Другие могут быть встроены в программы. Некоторые

же выполняются людьми и являются реализацией указаний руководства, содержащихся в соответствующих руководящих документах. Принятие решения о выборе уровня сложности технологий для защите системы требует установления критичности информации и последующего определения адекватного уровня безопасности.

Что же такое критические данные? Под критическими данными будем понимать данные, которые требуют защиты из-за вероятности нанесения(риска) ущерба и его величины в том случае, если произойдет случайное или умышленное раскрытие, изменение, или разрушение данных. Этот термин включает в себя данные, чье неправильное использование или раскрытие может отрицательно отразиться на способности организации решать свои задачи, персональные данные и другие данные, защита которых требуется указами Президента РФ, законами РФ и другими подзаконными документами.

Преступления и злоупотребления

Анализ зарубежных и отечественных отчетов о выявленных компьютерных преступлениях позволяет описать основные технологии их совершения. Лишь немногие из них включают разрушение компьютеров или данных. Только в 3 процентах мошенничеств и 8 процентах злоупотреблений происходило специальное разрушение оборудования, уничтожение программ или данных. В большей части случаев мошенничеств и злоупотреблений использовалась информация - ею манипулировали, ее создавали, ее использовали.

Пять основных технологий, использовавшихся при совершении компьютерных преступлений:

Мошенничества

1. Ввод неавторизованной информации
2. Манипуляции разрешенной для ввода информацией
3. Манипуляции или неправильное использование файлов с информацией
4. Создание неавторизованных файлов с информацией
5. Обход внутренних мер защиты

Злоупотребления

1. Кража компьютерного времени, программ, информации и оборудования
2. Ввод неавторизованной информации
3. Создание неавторизованных файлов с информацией
4. Разработка компьютерных программ для неслужебного использования
5. Манипулирование или неправильное использование возможностей по проведению работ на компьютерах

С другой стороны стоит рассмотреть основные методы, использовавшиеся для их совершения. Они включают:

1. **Надувательство с данными.** Наверное, самый распространенный метод при совершении компьютерных преступлений, так как он не требует технических знаний и относительно безопасен. Информация меняется в процессе ее ввода в компьютер или во время вывода. Например, при вводе документы могут быть заменены фальшивыми, вместо рабочих дискет подсунуты чужие, и данные могут быть сфальсифицированы.

2. **Сканирование.** Другой распространенный метод получения информации, который может привести к преступлению. Служащие, читающие файлы других, могут обнаружить там персональную информацию о своих коллегах. Информация, позволяющая получить доступ к компьютерным файлам или изменить их, может быть найдена после просмотра мусорных корзин. Дискеты, оставленные на столе, могут быть прочитаны, скопированы, и украдены. Очень хитрый сканирующий может даже просматривать остаточную информацию, оставшуюся на компьютере или на носителе информации после выполнения сотрудником задания и удаления своих файлов.

3. **Троянский конь.** Этот метод предполагает, что пользователь не заметил, что компьютерная программа была изменена таким образом, что включает в себя

дополнительные функции. Программа, выполняющая полезные функции, пишется таким образом, что содержит дополнительные скрытые функции, которые будут использовать особенности механизмов защиты системы(возможности пользователя, запустившего программу, по доступу к файлам)

4. **Люк.** Этот метод основан на использовании скрытого программного или аппаратного механизма, позволяющего обойти методы защиты в системе. Этот механизм активируется некоторым неочевидным образом. Иногда программа пишется таким образом, что специфическое событие, например, число транзакций, обработанных в определенный день, вызовет запуск неавторизованного механизма.

5. **Технология салями** Названа так из-за того, что преступление совершается понемногу, небольшими частями, настолько маленькими, что они незаметны. Обычно эта технология сопровождается изменением компьютерной программы. Например, платежи могут округляться до нескольких центов, и разница между реальной и округленной суммой поступать на специально открытый счет злоумышленника.

6. **Суперотключение**. Названа по имени программы, использовавшейся в ряде компьютерных центров, обходившей системные меры защиты и использовавшейся при аварийных ситуациях. Владение этим "мастер-ключом" дает возможность в любое время получить доступ к компьютеру и информации, находящейся в нем.

Признаки

Следующие признаки могут свидетельствовать о наличии уязвимых мест в информационной безопасности.

1. Не разработано положений о защите информации или они не соблюдаются. Не назначен ответственный за информационную безопасность.

2. Пароли пишутся на компьютерных терминалах, помещаются в общедоступные места, ими делятся с другими, или они появляются на компьютерном экране при их вводе

3. Удаленные терминалы и микрокомпьютеры оставляются без присмотра в рабочие и нерабочие часы. Данные отображаются на компьютерных экранах, оставленных без присмотра.

4. Не существует ограничений на доступ к информации, или на характер ее использования. Все пользователи имеют доступ ко всей информации и могут использовать все функции системы.

5. Не ведется системных журналов, и не хранится информация о том, кто и для чего использует компьютер.

6. Изменения в программы могут вноситься без их предварительного утверждения руководством.

7. Отсутствует документация или она не позволяет делать следующее: понимать получаемые отчеты и формулы, по которым получаются результаты, модифицировать программы, готовить данные для ввода, исправлять ошибки, производить оценку мер защиты, и понимать сами данные - их источники, формат хранения, взаимосвязи между ними.

8. Делаются многочисленные попытки войти в систему с неправильными паролями.

9. Вводимые данные не проверяются на корректность и точность, или при их проверке много данных отвергается из-за ошибок в них, требуется сделать много исправлений в данных, не делается записей в журналах об отвергнутых транзакциях.

10. Имеют место выходы из строя системы, приносящие большие убытки

11. Не производился анализ информации, обрабатываемой в компьютере, с целью определения необходимого для нее уровня безопасности

12. Мало внимания уделяется информационной безопасности. Хотя политика безопасности и существует, большинство людей считает, что на самом деле она не нужна.

МЕРЫ ЗАЩИТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1. **Контролируйте доступ как к информации в компьютере**, так и к прикладным программам. Вы должны иметь гарантии того, что только авторизованные пользователи имеют доступ к информации и приложениям.

Идентификация пользователей. Требуйте, чтобы пользователи выполняли процедуры входа в компьютер, и используйте это как средство для идентификации в начале работы. Чтобы эффективно контролировать микрокомпьютер, может оказаться наиболее выгодным использовать его как однопользовательскую систему. Обычно у микрокомпьютера нет процедур входа в систему, право использовать систему предоставляется простым включением компьютера.

Аутентификация пользователей. Используйте уникальные пароли для каждого пользователя, которые не являются комбинациями личных данных пользователей, для аутентификации личности пользователя. Внедрите меры защиты при администрировании паролей, и ознакомьте пользователей с наиболее общими ошибками, позволяющими совершиться компьютерному преступлению

Другие меры защиты:

Пароли - только один из типов идентификации - что-то, что знает только пользователь. Двумя другими типами идентификации, которые тоже эффективны, являются что-то, чем владеет пользователь(например, магнитная карта), или уникальные характеристики пользователя(его голос).

Если в компьютере имеется встроенный стандартный пароль(пароль, который встроен в программы и позволяет обойти меры по управлению доступом), обязательно измените его.

Сделайте так, чтобы программы в компьютере после входа пользователя в систему сообщали ему время его последнего сеанса и число неудачных попыток установления сеанса после этого. Это позволит сделать пользователя составной частью системы проверки журналов.

Защищайте ваш пароль

· не делитесь своим паролем ни с кем

· выбирайте пароль трудно угадываемым

· попробуйте использовать строчные и прописные буквы, цифры, или выберите знаменитое изречение и возьмите оттуда каждую четвертую букву. А еще лучше позвольте компьютеру самому сгенерировать ваш пароль.

· не используйте пароль, который является вашим адресом, псевдонимом, именем жены, телефонным номером или чем-либо очевидным.

· используйте длинные пароли, так как они более безопасны, лучше всего от 6 до 8 символов

· обеспечьте неотображаемость пароля на экране компьютера при его вводе

· обеспечьте отсутствие паролей в распечатках

· не записывайте пароли на столе, стене или терминале. Держите его в памяти

Серьезно относитесь к администрированию паролей

· периодически меняйте пароли и делайте это не по графику

· шифруйте или делайте что-нибудь еще с файлами паролей, хранящимися в компьютере, для защиты их от неавторизованного доступа.

· назначайте на должность администратора паролей только самого надежного человека

· не используйте один и тот же пароль для всех сотрудников в группе

· меняйте пароли, когда человек увольняется

· заставляйте людей расписываться за получение паролей

· установите и внедрите правила работы с паролями и обеспечьте, чтобы все знали их

Процедуры авторизации

Разработайте процедуры авторизации, которые определяют, кто из пользователей должен иметь доступ к той или иной информации и приложениям - и используйте соответствующие меры по внедрению этих процедур в организации.

Установите порядок в организации, при котором для использования компьютерных ресурсов, получения разрешения доступа к информации и приложениям, и получения пароля требуется разрешение тех или иных начальников.

Защита файлов

Помимо идентификации пользователей и процедур авторизации разработайте процедуры по ограничению доступа к файлам с данными:

· используйте внешние и внутренние метки файлов для указания типа информации, который они содержат, и требуемого уровня безопасности

· ограничьте доступ в помещения, в которых хранятся файлы данных, такие как архивы и библиотеки данных

· используйте организационные меры и программно-аппаратные средства для ограничения доступа к файлам только авторизованных пользователей

Предосторожности при работе

· отключайте неиспользуемые терминалы

· закрывайте комнаты, где находятся терминалы

· разворачивайте экраны компьютеров так, чтобы они не были видны со стороны двери, окон и тех мест в помещениях, которые не контролируются

· установите специальное оборудование, такое как устройства, ограничивающие число неудачных попыток доступа, или делающие обратный звонок для проверки личности пользователей, использующих телефоны для доступа к компьютеру

· программируйте терминал отключаться после определенного периода неиспользования

· если это возможно, выключайте систему в нерабочие часы

2. **Защищайте целостность информации.** Вводимая информация должна быть авторизована, полна, точна и должна подвергаться проверкам на ошибки.

Целостность информации

Проверяйте точность информации с помощью процедур сравнения результатов обработки с предполагаемыми результатами обработки. Например, можно сравнивать суммы или проверять последовательные номера.

Проверяйте точность вводимых данных, требуя от служащих выполнять проверки на корректность, такие как:

· проверки на нахождение символов в допустимом диапазоне символов(числовом или буквенном)

· проверки на нахождение числовых данных в допустимом диапазоне чисел

· проверки на корректность связей с другими данными, сравнивающими входные данные с данными в других файлах

· проверки на разумность, сравнивающие входные данные с ожидаемыми стандартными значениями

· ограничения на транзакции, сравнивающие входные данные с административно установленными ограничениями на конкретные транзакции

Трассируйте транзакции в системе

Делайте перекрестные проверки содержимого файлов с помощью сопоставления числа записей или контроля суммы значений поля записи.

3. **Защищайте системные программы.** Если ПО используется совместно, защищайте его от скрытой модификации при помощи политики безопасности, мер защиты при его разработке и контроле за ним в его жизненном цикле, а также обучения пользователей в области безопасности.

Меры защиты при разработке программ и соответствующие политики должны включать процедуры внесения изменений в программу, ее приемки и тестирования до

ввода в эксплуатацию. Политики должны требовать разрешения ответственного лица из руководства для внесения изменений в программы, ограничения списка лиц, кому разрешено вносить изменения и явно описывать обязанности сотрудников по ведению документации.

Должен быть разработан и поддерживаться каталог прикладных программ.

Должны быть внедрены меры защиты по предотвращению получения, изменения или добавления программ неавторизованными людьми через удаленные терминалы.

4. **Сделайте меры защиты более адекватными с помощью привлечения организаций**, занимающихся тестированием информационной безопасности, при разработке мер защиты в прикладных программах и консультируйтесь с ними при определении необходимости тестов и проверок при обработке критических данных. Контрольные журналы, встроенные в компьютерные программы, могут предотвратить или выявить компьютерное мошенничество и злоупотребление.

Должны иметься контрольные журналы для наблюдения за тем, кто из пользователей обновлял критические информационные файлы

Если критичность информации, хранимой в компьютерах, требует контрольных журналов, то важны как меры физической защиты, так и меры по управлению доступом.

В компьютерной сети журналы должны храниться на хосте, а не на рабочей станции.

Контрольные журналы не должны отключаться для повышения скорости работы.

Распечатки контрольных журналов должны просматриваться достаточно часто и регулярно.

5. **Рассмотрите вопрос о коммуникационной безопасности**. Данные, передаваемые по незащищенным линиям, могут быть перехвачены.

Физическая безопасность

Традиционная безопасность: замки, ограждение и охрана

Физическая безопасность означает лишь содержание компьютера и информации в нем в безопасности от физических опасностей с помощью замков на входах в помещение, где он находится, строительства ограждения вокруг зданий и размещения охраны вокруг помещения. Но физическая безопасность сейчас изменилась из-за современной компьютерной среды - среды, которая часто представляет собой офис с большим числом персональных ЭВМ или терминалов.

Физическая безопасность связана с внедрением мер защиты, которые защищают от стихийных бедствий(пожаров, наводнений, и землетрясений), а также всяких случайных инцидентов. Меры физической безопасности определяют, каким будет окружение компьютера, вводимые данные, и результаты обработки информации. Помимо помещений, где размещено компьютерное оборудование, окружение включает в себя библиотеки программ, журналы, магнитные носители, помещения для архивов, и помещения для ремонта техники.

Меры физической защиты должны отвечать требованиям современной действительности и сочетать эффективность с невысокой ценой. Например, установка дорогой противопожарной системы может быть необходимой для защиты большого компьютера, обрабатывающего критические данные, но оказаться неоправданно дорогой при защите одной персональной ЭВМ.

Преступления и злоупотребления

Компьютеры могут быть повреждены, украдены и специально выведены из строя с помощью короткого замыкания. Диски и ленты могут быть разрушены разлитыми напитками, а компьютеры залиты водой. Также компьютеры могут быть серьезно повреждены пожаром, скачками напряжения, стихийными бедствиями и другими инцидентами. Информация может быть перехвачена, украдена, продана и использоваться в корыстных целях отдельным человеком или целой компанией.

Персональные ЭВМ особенно привлекают воров. При пожаре диски, не хранящиеся в специальных сейфах или флоппи-диски, оставленные на терминалах, могут быть

разрушены системой тушения пожара. Тысячи долларов были потрачены на восстановление информации, которую они содержали.

Но основной причиной разрушений компьютеров является, судя по всему, обычная неосторожность людей и вредное влияние окружающей среды.

Признаки

Следующие признаки могут указывать на наличие уязвимых мест в физической безопасности:

· разрешено курить, есть и пить рядом с компьютерами

· компьютерное оборудование оставляется в незапертых комнатах или является незащищенным по какой-либо другой причине

· не установлена пожарная сигнализация

· диски оставляются в ящиках столов, не делается архивных копий дисков

· посетителям не задается вопросов о причине их нахождения в помещениях, где установлены компьютеры

· реестр компьютерного оборудования и программ отсутствует, неполон, не обновляется или не проверяется после его заполнения.

· распечатки, микрофиши, диски, содержащие критические данные выбрасываются в обычное мусорное ведро

· замки на входах в помещения, где находится компьютерное оборудование, никогда не менялись

· не производилось аттестации автоматизированной системы организации, то есть анализа насколько она уязвима к доступу неавторизованных людей, пожару или наводнению.

Меры физической безопасности

1.Предотвратить злонамеренные разрушения, неавторизованное использование или кражу

ПЭВМ могут быть заперты в комнатах и доступ к ним может быть ограничен с помощью устройств блокировки клавиатуры и т.п. Удостоверьтесь, что люди соблюдают свои обязанности по использованию компьютеров и их можно проконтролировать.

Если информация обрабатывается на большом вычислительном центре, проверьте, как контролируется физический доступ к вычислительной технике. Могут оказаться уместными такие методы, как журналы, замки и пропуска, а также охрана.

Ввод критической информации требует правильного обращения с исходными документами. Правильное обращение означает соблюдение одинаковых правил работы с документами, независимо от того, используются они в автоматизированной системе или нет. Правила работы могут включать работу в безопасном помещении, учет документов в журналах, гарантии того, что только люди, имеющие соответствующий допуск, могут ознакомиться с этими документами, и использование устройств уничтожения документов (бумагорезок и т.п.).

Внимательно проанализируйте размещение компьютеров. Не слишком ли доступны они неавторизованным людям или чрезмерно уязвимы к стихийным бедствиям?

Вы должны иметь представление об основных схемах сопровождения посторонних. Например, авторизованный сотрудник должен сопровождать в компьютерной зоне посетителя с компьютерными распечатками или человека, заявляющего, что он техник по ремонту компьютеров.

Вы должны знать, кто имеет право доступа в помещения с компьютерным оборудованием и выгонять оттуда посторонних лиц.

Многие люди полагают, что двери, оснащенные замками и охраняемые людьми, обеспечивают физическую безопасность. Но электромагнитные излучения от компьютеров могут быть перехвачены и таким образом может быть прочитана информация с экрана. Рекомендуемые меры защиты от этого должны учитывать

требуемый уровень безопасности и тот факт, что такой перехват крайне редок, но может и произойти.

Могут быть предприняты недорогие предохранительные меры , которые будут гарантировать, что телефонные и компьютерные каналы связи в состоянии выполнять свои функции и являются безопасными. В сети может потребоваться выделенный канал связи - он не выполняет других функций. С другой стороны выделение персональной ЭВМ для работы на ней одного приложения может оказаться самым эффективным средством защиты.

Для любой из основных трех технологий для передачи автоматизированной информации существует технология перехвата : кабель(подключение к кабелю), спутник(антенна приема сигнала со спутника), радиоволны(радиоперехват).

Технологии защиты, которые могут быть использованы, включают шифрование информации, использование выделенных линий, модемы с функциям безопасности, и использование скремблирования голосовых переговоров.

2. Стихийные бедствия могут нанести большой ущерб как большим, так и маленьким компаниям.

Примите меры по предотвращению, обнаружению и минимизации ущерба от пожара, наводнения, загрязнения окружающей среды, высоких температур и скачков напряжения.

Защищайтесь от пожара с помощью регулярной проверки пожарной сигнализации и систем пожаротушения. Защищайте ПЭВМ с помощью кожухов, чтобы они не были повреждены системой пожаротушения. Не храните горючие материалы в этих помещениях.

Статическое электричество может очистить память в ПЭВМ. Антистатические коврики могут предотвратить это. Пользователям следует напоминать о снятии заряда с себя с помощью прикосновения к заземленному объекту.

Скачки напряжения могут очистить память, изменить программы и разрушить микросхемы. Устройство бесперебойного питания(УБП) дает достаточно времени, чтобы отключить компьютер без потери данных. Предохранить компьютеры от кратковременных бросков питания могут фильтры напряжения. В грозу незащищенные ПЭВМ могут быть отключены и выключены из сети.

Температура в помещении может контролироваться кондиционерами и вентиляторами, а также хорошей вентиляцией в помещении. Проблемы с чрезмерно высокой температурой могут возникнуть в стойках периферийного оборудования или из-за закрытия вентиляционного отверстия в терминалах или ПЭВМ.

Воздушные фильтры могут очистить воздух от вредных веществ в нем, которые могут нанести вред компьютерам и дискам. Следует запретить курить возле ПЭВМ.

Размещайте компьютеры подальше от того, что может явиться источником большого количества воды, например трубопроводов, обычно затапливаемых помещений или не используйте систему пожаротушения, если есть другие способы защиты от пожара.

Держите еду и напитки подальше от компьютера.

Содержите оборудование в порядке. Следите и учитывайте в журналах ремонт техники. Это позволит проконтролировать, кто имел доступ к системе. Помните, что бригады ремонтников должны производить правильную идентификацию себя.

3. Защищайте все носители информации(исходные документы, ленты, картриджи, диски, распечатки)

· ведите, контролируйте и проверяйте реестры носителей информации

· обучайте пользователей правильным методам очищения и уничтожения носителей информации

· делайте метки на носителях информации, отражающие уровень критичности информации, которая в них содержится.

· уничтожайте носители информации в соответствии с планом организации

· удостоверьтесь, что доступ к носителям информации для их хранения, передачи, нанесения меток, и уничтожения предоставлен только авторизованным людям

· доведите все руководящие документы до сотрудников

Подумайте о возможности публикации следующих рекомендаций в общедоступном месте:

Диски уязвимы

· храните их в конвертах и коробках

· не пишите на конвертах

· не гните их

· не касайтесь самих дисков

· осторожно вставляйте их в компьютер

· не разливайте на них напитки

· держите их подальше от источников магнитного поля

· храните их в металлических сейфах

· работайте с дисками в соответствии с маркировкой критичности на них

Правильное обращение обеспечивает защиту

· убирайте диски и ленты, когда не работаете с ними

· храните их разложенными по полкам в определенном порядке

· не давайте носители информации с критической информацией неавторизованным людям

· отдавайте поврежденные диски с критической информацией только после их размагничивания или аналогичной процедуры

· уничтожайте критическую информацию на дисках с помощью их размагничивания или физического разрушения в соответствии с порядком в вашей организации

· уничтожайте распечатки и красящие ленты от принтеров с критической информацией в соответствии с порядком в вашей организации.

· обеспечьте безопасность распечаток паролей и другой информации, позволяющей получить доступ к компьютеру

4. Удостоверьтесь, что существуют адекватные планы действий при ЧП(планы обеспечения непрерывной работы). Помните, что целью этих планов являются гарантии того, что пользователи смогут продолжать выполнять самые главные свои обязанности в случае невозможности работы по информационной технологии. Конечные пользователи информационной технологии, а также обслуживающий персонал, должны знать, как им действовать по этим планам.

Планы обеспечения непрерывной работы и восстановления (ОНРВ) должны быть написаны, проверены и регулярно доводиться до сотрудников.

ОНРВ должны учитывать наличие операций архивации, то есть как будет обрабатываться информация, если компьютеры, на которых она обрабатывалась обычно, нельзя использовать, и необходимость восстановления потерянной или разрушенной информации.

Особенно для ПЭВМ ОНРВ должны учитывать выход из строя той или иной техники, например выход из строя сетевого принтера.

Процедуры и техника должны планироваться в расчете на пожар, затопление и т.д.

Храните архивные копии, включая план ОНРВ, в безопасном месте, удаленном от основных помещений, занимаемых компьютерами.

Процедуры плана должны быть адекватны уровню безопасности и критичности информации.

Знайте, что делать в случае ЧП, и будьте знакомы с планом ОНРВ Помните, что план ОНРВ может применяться в условиях неразберихи и паники. Тренировки ваших сотрудников жизненно необходимы.

Информационная безопасность в Intranet

Архитектура Intranet подразумевает подключение к внешним открытым сетям, использование внешних сервисов и предоставление собственных сервисов вовне, что предъявляет повышенные требования к защите информации.

В Intranet-системах используется подход клиент-сервер, а главная роль на сегодняшний день отводится Web-сервису. Web-серверы должны поддерживать традиционные защитные средства, такие как аутентификация и разграничение доступа; кроме того, необходимо обеспечение новых свойств, в особенности безопасности программной среды и на серверной, и на клиентской сторонах.

Таковы, если говорить совсем кратко, задачи в области информационной безопасности, возникающие в связи с переходом на технологию Intranet. Далее мы рассмотрим возможные подходы к их решению.

Позволю себе небольшое отступление. Некоторое время назад один мой знакомый банкир, прочитав в каком-то дорогом журнале статью об информационной безопасности, сделал для себя вывод, что защищаться бесполезно - слишком велик арсенал потенциального злоумышленника. Он перестал рассматривать предложения по защите компьютерной системы банка, считая их заведомо бесполезными. К фаталистам моего знакомого не отнесешь, от подтяжек он еще не отказался, однако масса технических деталей, приведенных в журнальной статье, совершенно запутала и подавила его. Сжав голову руками, он ходил из угла в угол, бормоча: "Пароли перехватываются, соединения крадутся, получить привилегии root - раз плюнуть" и т.д. и т.п. Мои попытки указать ему на то, что в статье допущен ряд чисто технических ошибок, что не оговорены условия, при которых возможна та или иная атака, что, наконец, отсутствует комплексный подход к проблеме безопасности, успеха не имели.

Так совпало, что вскоре дела банка, где работал мой знакомый, стали идти все хуже и хуже. Более удачливые конкуренты, казалось, все время предугадывали его ходы, постоянно оказываясь на полшага впереди. Надеюсь, что у читателей журнала LAN Magazine, напротив, все пойдет как нельзя лучше и у них окажется больше здравого смысла, больше умения видеть проблему в целом.

Формирование режима информационной безопасности - проблема комплексная. Меры по ее решению можно разделить на четыре уровня:

законодательный (законы, нормативные акты, стандарты и т.п.); административный (действия общего характера, предпринимаемые руководством организации); процедурный (конкретные меры безопасности, имеющие дело с людьми); программно-технический (конкретные технические меры).

В таком порядке и будет построено последующее изложение.

Законодательный уровень

В настоящее время наиболее подробным законодательным документом в области информационной безопасности является Уголовный кодекс, точнее говоря, его новая редакция, вступившая в силу в мае 1996 года.

В разделе IX ("Преступления против общественной безопасности") имеется глава 28 - "Преступления в сфере компьютерной информации". Она содержит три статьи - 272 ("Неправомерный доступ к компьютерной информации"), 273 ("Создание, использование и распространение вредоносных программ для ЭВМ") и 274 - "Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети". Уголовный кодекс стоит на страже всех аспектов информационной безопасности - доступности, целостности, конфиденциальности, предусматривая наказания за "уничтожение, блокирование, модификацию и копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети".

Весьма энергичную работу в области современных информационных технологий проводит Государственная техническая комиссия (Гостехкомиссия) при Президенте Российской Федерации. В рамках серии руководящих документов (РД) Гостехкомиссии подготовлен проект РД, устанавливающий классификацию межсетевых экранов (firewalls,

или брандмауэров) по уровню обеспечения защищенности от несанкционированного доступа (НСД). Это принципиально важный документ, позволяющий упорядочить использование защитных средств, необходимых для реализации технологии Intranet.

Разработка сетевых аспектов политики безопасности

Политика безопасности определяется как совокупность документированных управленческих решений, направленных на защиту информации и ассоциированных с ней ресурсов.

При разработке и проведении ее в жизнь целесообразно руководствоваться следующими принципами:

невозможность миновать защитные средства; усиление самого слабого звена; невозможность перехода в небезопасное состояние; минимизация привилегий; разделение обязанностей; эшелонированность обороны; разнообразие защитных средств; простота и управляемость информационной системы; обеспечение всеобщей поддержки мер безопасности.

Поясним смысл перечисленных принципов.

Если у злоумышленника или недовольного пользователя появится возможность миновать защитные средства, он, разумеется, так и сделает. Применительно к межсетевым экранам данный принцип означает, что все информационные потоки в защищаемую сеть и из нее должны проходить через экран. Не должно быть "тайных" модемных входов или тестовых линий, идущих в обход экрана.

Надежность любой обороны определяется самым слабым звеном. Злоумышленник не будет бороться против силы, он предпочтет легкую победу над слабостью. Часто самым слабым звеном оказывается не компьютер или программа, а человек, и тогда проблема обеспечения информационной безопасности приобретает нетехнический характер.

Принцип невозможности перехода в небезопасное состояние означает, что при любых обстоятельствах, в том числе нештатных, защитное средство либо полностью выполняет свои функции, либо полностью блокирует доступ. Образно говоря, если в крепости механизм подъемного моста ломается, мост должен оставаться в поднятом состоянии, препятствуя проходу неприятеля.

Принцип минимизации привилегий предписывает выделять пользователям и администраторам только те права доступа, которые необходимы им для выполнения служебных обязанностей.

Принцип разделения обязанностей предполагает такое распределение ролей и ответственности, при котором один человек не может нарушить критически важный для организации процесс. Это особенно важно, чтобы предотвратить злонамеренные или неквалифицированные действия системного администратора.

Принцип эшелонированности обороны предписывает не полагаться на один защитный рубеж, каким бы надежным он ни казался. За средствами физической защиты должны следовать программно-технические средства, за идентификацией и аутентификацией - управление доступом и, как последний рубеж, - протоколирование и аудит. Эшелонированная оборона способна по крайней мере задержать злоумышленника, а наличие такого рубежа, как протоколирование и аудит, существенно затрудняет незаметное выполнение злоумышленных действий.

Принцип разнообразия защитных средств рекомендует организовывать различные по своему характеру оборонительные рубежи, чтобы от потенциального злоумышленника требовалось овладение разнообразными и, по возможности, несовместимыми между собой навыками (например умением преодолевать высокую ограду и знанием слабостей нескольких операционных систем).

Очень важен принцип простоты и управляемости информационной системы в целом и защитных средств в особенности. Только для простого защитного средства можно формально или неформально доказать его корректность. Только в простой и управляемой

системе можно проверить согласованность конфигурации разных компонентов и осуществить централизованное администрирование. В этой связи важно отметить интегрирующую роль Web-сервиса, скрывающего разнообразие обслуживаемых объектов и предоставляющего единый, наглядный интерфейс. Соответственно, если объекты некоторого вида (скажем таблицы базы данных) доступны через Web, необходимо заблокировать прямой доступ к ним, поскольку в противном случае система будет сложной и трудноуправляемой.

Последний принцип - всеобщая поддержка мер безопасности - носит нетехнический характер. Если пользователи и/или системные администраторы считают информационную безопасность чем-то излишним или даже враждебным, режим безопасности сформировать заведомо не удастся. Следует с самого начала предусмотреть комплекс мер, направленный на обеспечение лояльности персонала, на постоянное обучение, теоретическое и, главное, практическое.

Анализ рисков - важнейший этап выработки политики безопасности. При оценке рисков, которым подвержены Intranet-системы, нужно учитывать следующие обстоятельства:

новые угрозы по отношению к старым сервисам, вытекающие из возможности пассивного или активного прослушивания сети. Пассивное прослушивание означает чтение сетевого трафика, а активное - его изменение (кражу, дублирование или модификацию передаваемых данных). Например, аутентификация удаленного клиента с помощью пароля многократного использования не может считаться надежной в сетевой среде, независимо от длины пароля; новые (сетевые) сервисы и ассоциированные с ними угрозы.

Как правило, в Intranet-системах следует придерживаться принципа "все, что не разрешено, запрещено", поскольку "лишний" сетевой сервис может предоставить канал проникновения в корпоративную систему. В принципе, ту же мысль выражает положение "все непонятное опасно".

Процедурные меры

В общем и целом Intranet-технология не предъявляет каких-либо специфических требований к мерам процедурного уровня. На наш взгляд, отдельного рассмотрения заслуживают лишь два обстоятельства:

описание должностей, связанных с определением, наполнением и поддержанием корпоративной гипертекстовой структуры официальных документов; поддержка жизненного цикла информации, наполняющей Intranet.

При описании должностей целесообразно исходить из аналогии между Intranet и издательством. В издательстве существует директор, определяющий общую направленность деятельности. В Intranet ему соответствует Web-администратор, решающий, какая корпоративная информация должна присутствовать на Web-сервере и как следует структурировать дерево (точнее, граф) HTML-документов.

В многопрофильных издательствах существуют редакции, занимающиеся конкретными направлениями (математические книги, книги для детей и т.п.). Аналогично, в Intranet целесообразно выделить должность публикатора, ведающего появлением документов отдельных подразделений и определяющего перечень и характер публикаций.

У каждой книги есть титульный редактор, отвечающий перед издательством за свою работу. В Intranet редакторы занимаются вставкой документов в корпоративное дерево, их коррекцией и удалением. В больших организациях "слой" публикатор/редактор может состоять из нескольких уровней.

Наконец, и в издательстве, и в Intranet должны быть авторы, создающие документы. Подчеркнем, что они не должны иметь прав на модификацию корпоративного дерева и отдельных документов. Их дело - передать свой труд редактору.

Кроме официальных, корпоративных, в Intranet могут присутствовать групповые и личные документы, порядок работы с которыми (роли, права доступа) определяется, соответственно, групповыми и личными интересами.

Переходя к вопросам поддержки жизненного цикла Intranet-информации, напомним о необходимости использования средств конфигурационного управления. Важное достоинство Intranet-технологии состоит в том, что основные операции конфигурационного управления - внесение изменений (создание новой версии) и извлечение старой версии документа - естественным образом вписываются в рамки Web-интерфейса. Те, для кого это необходимо, могут работать с деревом всех версий всех документов, подмножеством которого является дерево самых свежих версий.

Управление доступом путем фильтрации информации

Мы переходим к рассмотрению мер программно-технического уровня, направленных на обеспечение информационной безопасности систем, построенных в технологии Intranet. На первое место среди таких мер мы поставим межсетевые экраны - средство разграничения доступа, служащее для защиты от внешних угроз и от угроз со стороны пользователей других сегментов корпоративных сетей.

Отметим, что бороться с угрозами, присущими сетевой среде, средствами универсальных операционных систем не представляется возможным. Универсальная ОС - это огромная программа, наверняка содержащая, помимо явных ошибок, некоторые особенности, которые могут быть использованы для получения нелегальных привилегий. Современная технология программирования не позволяет сделать столь большие программы безопасными. Кроме того, администратор, имеющий дело со сложной системой, далеко не всегда в состоянии учесть все последствия производимых изменений (как и врач, не ведающий всех побочных воздействий рекомендуемых лекарств). Наконец, в универсальной многопользовательской системе бреши в безопасности постоянно создаются самими пользователями (слабые и/или редко изменяемые пароли, неудачно установленные права доступа, оставленный без присмотра терминал и т.п.).

Как указывалось выше, единственный перспективный путь связан с разработкой специализированных защитных средств, которые в силу своей простоты допускают формальную или неформальную верификацию. Межсетевой экран как раз и является таким средством, допускающим дальнейшую декомпозицию, связанную с обслуживанием различных сетевых протоколов.

Межсетевой экран - это полупроницаемая мембрана, которая располагается между защищаемой (внутренней) сетью и внешней средой (внешними сетями или другими сегментами корпоративной сети) и контролирует все информационные потоки во внутреннюю сеть и из нее (Рис. 2). Контроль информационных потоков состоит в их фильтрации, то есть в выборочном пропускании через экран, возможно, с выполнением некоторых преобразований и извещением отправителя о том, что его данным в пропуске отказано. Фильтрация осуществляется на основе набора правил, предварительно загруженных в экран и являющихся выражением сетевых аспектов политики безопасности организации.

Целесообразно разделить случаи, когда экран устанавливается на границе с внешней (обычно общедоступной) сетью или на границе между сегментами одной корпоративной сети. Соответственно, мы будет говорить о внешнем и внутреннем межсетевых экранах.

Как правило, при общении с внешними сетями используется исключительно семейство протоколов TCP/IP. Поэтому внешний межсетевой экран должен учитывать специфику этих протоколов. Для внутренних экранов ситуация сложнее, здесь следует принимать во внимание помимо TCP/IP по крайней мере протоколы SPX/IPX, применяемые в сетях Novell NetWare. Иными словами, от внутренних экранов нередко требуется многопротокольность.

Ситуации, когда корпоративная сеть содержит лишь один внешний канал, является, скорее, исключением, чем правилом. Напротив, типична ситуация, при которой

корпоративная сеть состоит из нескольких территориально разнесенных сегментов, каждый из которых подключен к сети общего пользования (Рис. 3). В этом случае каждое подключение должно защищаться своим экраном. Точнее говоря, можно считать, что корпоративный внешний межсетевой экран является составным, и требуется решать задачу согласованного администрирования (управления и аудита) всех компонентов. Экранирование корпоративной сети, состоящей из нескольких территориально разнесенных сегментов, каждый из которых подключен к сети общего пользования.

При рассмотрении любого вопроса, касающегося сетевых технологий, основой служит семиуровневая эталонная модель ISO/OSI. Межсетевые экраны также целесообразно классифицировать по тому, на каком уровне производится фильтрация - канальном, сетевом, транспортном или прикладном. Соответственно, можно говорить об экранирующих концентраторах (уровень 2), маршрутизаторах (уровень 3), о транспортном экранировании (уровень 4) и о прикладных экранах (уровень 7). Существуют также комплексные экраны, анализирующие информацию на нескольких уровнях.

В данной работе мы не будем рассматривать экранирующие концентраторы, поскольку концептуально они мало отличаются от экранирующих маршрутизаторов.

При принятии решения "пропустить/не пропустить", межсетевые экраны могут использовать не только информацию, содержащуюся в фильтруемых потоках, но и данные, полученные из окружения, например текущее время.

Таким образом, возможности межсетевого экрана непосредственно определяются тем, какая информация может использоваться в правилах фильтрации и какова может быть мощность наборов правил. Вообще говоря, чем выше уровень в модели ISO/OSI, на котором функционирует экран, тем более содержательная информация ему доступна и, следовательно, тем тоньше и надежнее экран может быть сконфигурирован. В то же время фильтрация на каждом из перечисленных выше уровней обладает своими достоинствами, такими как дешевизна, высокая эффективность или прозрачность для пользователей. В силу этой, а также некоторых других причин, в большинстве случаев используются смешанные конфигурации, в которых объединены разнотипные экраны. Наиболее типичным является сочетание экранирующих маршрутизаторов и прикладного экрана (Рис. 4).

Приведенная конфигурация называется экранирующей подсетью. Как правило, сервисы, которые организация предоставляет для внешнего применения (например "представительский" Web-сервер), целесообразно выносить как раз в экранирующую подсеть.

Помимо выразительных возможностей и допустимого количества правил качество межсетевого экрана определяется еще двумя очень важными характеристиками - простотой применения и собственной защищенностью. В плане простоты использования первостепенное значение имеют наглядный интерфейс при задании правил фильтрации и возможность централизованного администрирования составных конфигураций. В свою очередь, в последнем аспекте хотелось бы выделить средства централизованной загрузки правил фильтрации и проверки набора правил на непротиворечивость. Важен и централизованный сбор и анализ регистрационной информации, а также получение сигналов о попытках выполнения действий, запрещенных политикой безопасности.

Собственная защищенность межсетевого экрана обеспечивается теми же средствами, что и защищенность универсальных систем. При выполнении централизованного администрирования следует еще позаботиться о защите информации от пассивного и активного прослушивания сети, то есть обеспечить ее (информации) целостность и конфиденциальность.

Хотелось бы подчеркнуть, что природа экранирования (фильтрации), как механизма безопасности, очень глубока. Помимо блокирования потоков данных, нарушающих политику безопасности, межсетевой экран может скрывать информацию о защищаемой сети, тем самым затрудняя действия потенциальных злоумышленников. Так, прикладной

экран может осуществлять действия от имени субъектов внутренней сети, в результате чего из внешней сети кажется, что имеет место взаимодействие исключительно с межсетевым экраном (Рис. 5). При таком подходе топология внутренней сети скрыта от внешних пользователей, поэтому задача злоумышленника существенно усложняется.

Более общим методом сокрытия информации о топологии защищаемой сети является трансляция "внутренних" сетевых адресов, которая попутно решает проблему расширения адресного пространства, выделенного организации.

Ограничивающий интерфейс также можно рассматривать как разновидность экранирования. На невидимый объект трудно нападать, особенно с помощью фиксированного набора средств. В этом смысле Web-интерфейс обладает естественной защитой, особенно в том случае, когда гипертекстовые документы формируются динамически. Каждый видит лишь то, что ему положено.

Экранирующая роль Web-сервиса наглядно проявляется и тогда, когда этот сервис осуществляет посреднические (точнее, интегрирующие) функции при доступе к другим ресурсам, в частности таблицам базы данных. Здесь не только контролируются потоки запросов, но и скрывается реальная организация баз данных.

Безопасность программной среды

Идея сетей с так называемыми активными агентами, когда между компьютерами передаются не только пассивные, но и активные исполняемые данные (то есть программы), разумеется, не нова. Первоначально цель состояла в том, чтобы уменьшить сетевой трафик, выполняя основную часть обработки там, где располагаются данные (приближение программ к данным). На практике это означало перемещение программ на серверы. Классический пример реализации подобного подхода - это хранимые процедуры в реляционных СУБД.

Для Web-серверов аналогом хранимых процедур являются программы, обслуживающие общий шлюзовый интерфейс (Common Gateway Interface - CGI). CGI-процедуры располагаются на серверах и обычно используются для динамического порождения HTML-документов. Политика безопасности организации и процедурные меры должны определять, кто имеет право помещать на сервер CGI-процедуры. Жесткий контроль здесь необходим, поскольку выполнение сервером некорректной программы может привести к сколь угодно тяжелым последствиям. Разумная мера технического характера состоит в минимизации привилегий пользователя, от имени которого выполняется Web-сервер.

В технологии Intranet, если заботиться о качестве и выразительной силе пользовательского интерфейса, возникает нужда в перемещении программ с Web-серверов на клиентские компьютеры - для создания анимации, выполнения семантического контроля при вводе данных и т.д. Вообще, активные агенты - неотъемлемая часть технологии Intranet.

В каком бы направлении ни перемещались программы по сети, эти действия представляют повышенную опасность, т.к. программа, полученная из ненадежного источника, может содержать непреднамеренно внесенные ошибки или целенаправленно созданный зловредный код. Такая программа потенциально угрожает всем основным аспектам информационной безопасности:

доступности (программа может поглотить все наличные ресурсы); целостности (программа может удалить или повредить данные); конфиденциальности (программа может прочитать данные и передать их по сети).

Проблему ненадежных программ осознавали давно, но, пожалуй, только в рамках системы программирования Java впервые предложена целостная концепция ее решения.

Java предлагает три оборонительных рубежа:

надежность языка; контроль при получении программ; контроль при выполнении программ.

Впрочем, существует еще одно, очень важное средство обеспечения информационной безопасности - беспрецедентная открытость Java-системы. Исходные тексты Java-компилятора и интерпретатора доступны для проверки, поэтому велика вероятность, что ошибки и недочеты первыми будут обнаруживать честные специалисты, а не злоумышленники.

В концептуальном плане наибольшие трудности представляет контролируемое выполнение программ, загруженных по сети. Прежде всего, необходимо определить, какие действия считаются для таких программ допустимыми. Если исходить из того, что Java - это язык для написания клиентских частей приложений, одним из основных требований к которым является мобильность, загруженная программа может обслуживать только пользовательский интерфейс и осуществлять сетевое взаимодействие с сервером. Программа не может работать с файлами хотя бы потому, что на Java-терминале их, возможно, не будет. Более содержательные действия должны производиться на серверной стороне или осуществляться программами, локальными для клиентской системы.

Интересный подход предлагают специалисты компании Sun Microsystems для обеспечения безопасного выполнения командных файлов. Речь идет о среде Safe-Tcl (Tool Comman Language, инструментальный командный язык). Sun предложила так называемую ячеечную модель интерпретации командных файлов. Существует главный интерпретатор, которому доступны все возможности языка. Если в процессе работы приложения необходимо выполнить сомнительный командный файл, порождается подчиненный командный интерпретатор, обладающий ограниченной функциональностью (например, из него могут быть удалены средства работы с файлами и сетевые возможности). В результате потенциально опасные программы оказываются заключенными в ячейки, защищающие пользовательские системы от враждебных действий. Для выполнения действий, которые считаются привилегированными, подчиненный интерпретатор может обращаться с запросами к главному. Здесь, очевидно, просматривается аналогия с разделением адресных пространств операционной системы и пользовательских процессов и использованием последними системных вызовов. Подобная модель уже около 30 лет является стандартной для многопользовательских ОС.

Защита web-серверов

Наряду с обеспечением безопасности программной среды (см. предыдущий раздел), важнейшим будет вопрос о разграничении доступа к объектам Web-сервиса. Для решения этого вопроса необходимо уяснить, что является объектом, как идентифицируются субъекты и какая модель управления доступом - принудительная или произвольная - применяется.

В Web-серверах объектами доступа выступают универсальные локаторы ресурсов (URL - Uniform (Universal) Resource Locator). За этими локаторами могут стоять различные сущности - HTML-файлы, CGI-процедуры и т.п.

Как правило, субъекты доступа идентифицируются по IP-адресам и/или именам компьютеров и областей управления. Кроме того, может использоваться парольная аутентификация пользователей или более сложные схемы, основанные на криптографических технологиях (см. следующий раздел).

В большинстве Web-серверов права разграничиваются с точностью до каталогов (директорий) с применением произвольного управления доступом. Могут предоставляться права на чтение HTML-файлов, выполнение CGI-процедур и т.д.

Для раннего выявления попыток нелегального проникновения в Web-сервер важен регулярный анализ регистрационной информации.

Разумеется, защита системы, на которой функционирует Web-сервер, должна следовать универсальным рекомендациям, главной из которых является максимальное упрощение. Все ненужные сервисы, файлы, устройства должны быть удалены. Число пользователей, имеющих прямой доступ к серверу, должно быть сведено к минимуму, а их привилегии - упорядочены в соответствии со служебными обязанностями.

Еще один общий принцип состоит в том, чтобы минимизировать объем информации о сервере, которую могут получить пользователи. Многие серверы в случае обращения по имени каталога и отсутствия файла index.HTML в нем, выдают HTML-вариант оглавления каталога. В этом оглавлении могут встретиться имена файлов с исходными текстами CGI-процедур или с иной конфиденциальной информацией. Такого рода "дополнительные возможности" целесообразно отключать, поскольку лишнее знание (злоумышленника) умножает печали (владельца сервера).

Аутентификация в открытых сетях

Методы, применяемые в открытых сетях для подтверждения и проверки подлинности субъектов, должны быть устойчивы к пассивному и активному прослушиванию сети. Суть их сводится к следующему.

Субъект демонстрирует знание секретного ключа, при этом ключ либо вообще не передается по сети, либо передается в зашифрованном виде. Субъект демонстрирует обладание программным или аппаратным средством генерации одноразовых паролей или средством, работающим в режиме "запрос-ответ". Нетрудно заметить, что перехват и последующее воспроизведение одноразового пароля или ответа на запрос ничего не дает злоумышленнику. Субъект демонстрирует подлинность своего местоположения, при этом используется система навигационных спутников.

Виртуальные частные сети

Одной из важнейших задач является защита потоков корпоративных данных, передаваемых по открытым сетям. Открытые каналы могут быть надежно защищены лишь одним методом - криптографическим.

Отметим, что так называемые выделенные линии не обладают особыми преимуществами перед линиями общего пользования в плане информационной безопасности. Выделенные линии хотя бы частично будут располагаться в неконтролируемой зоне, где их могут повредить или осуществить к ним несанкционированное подключение. Единственное реальное достоинство - это гарантированная пропускная способность выделенных линий, а вовсе не какая-то повышенная защищенность. Впрочем, современные оптоволоконные каналы способны удовлетворить потребности многих абонентов, поэтому и указанное достоинство не всегда облечено в реальную форму.

Любопытно упомянуть, что в мирное время 95% трафика Министерства обороны США передается через сети общего пользования (в частности через Internet). В военное время эта доля должна составлять "лишь" 70%. Можно предположить, что Пентагон - не самая бедная организация. Американские военные полагаются на сети общего пользования потому, что развивать собственную инфраструктуру в условиях быстрых технологических изменений - занятие очень дорогое и бесперспективное, оправданное даже для критически важных национальных организаций только в исключительных случаях.

Представляется естественным возложить на межсетевой экран задачу шифрования и дешифрования корпоративного трафика на пути во внешнюю сеть и из нее. Чтобы такое шифрование/дешифрование стало возможным, должно произойти начальное распределение ключей. Современные криптографические технологии предлагают для этого целый ряд методов.

После того как межсетевые экраны осуществили криптографическое закрытие корпоративных потоков данных, территориальная разнесенность сегментов сети проявляется лишь в разной скорости обмена с разными сегментами. В остальном вся сеть выглядит как единое целое, а от абонентов не требуется привлечение каких-либо дополнительных защитных средств.

Простота и однородность архитектуры

Важнейшим аспектом информационной безопасности является управляемость системы. Управляемость - это и поддержание высокой доступности системы за счет

раннего выявления и ликвидации проблем, и возможность изменения аппаратной и программной конфигурации в соответствии с изменившимися условиями или потребностями, и оповещение о попытках нарушения информационной безопасности практически в реальном времени, и снижение числа ошибок администрирования, и многое, многое другое.

Наиболее остро проблема управляемости встает на клиентских рабочих местах и на стыке клиентской и серверной частей информационной системы. Причина проста - клиентских мест гораздо больше, чем серверных, они, как правило, разбросаны по значительно большей площади, их используют люди с разной квалификацией и привычками. Обслуживание и администрирование клиентских рабочих мест - занятие чрезвычайно сложное, дорогое и чреватое ошибками. Технология Intranet за счет простоты и однородности архитектуры позволяет сделать стоимость администрирования клиентского рабочего места практически нулевой. Важно и то, что замена и повторный ввод в эксплуатацию клиентского компьютера могут быть осуществлены очень быстро, поскольку это "клиенты без состояния", у них нет ничего, что требовало бы длительного восстановления или конфигурирования.

На стыке клиентской и серверной частей Intranet-системы находится Web-сервер. Это позволяет иметь единый механизм регистрации пользователей и наделения их правами доступа с последующим централизованным администрированием. Взаимодействие с многочисленными разнородными сервисами оказывается скрытым не только от пользователей, но и в значительной степени от системного администратора.

Заключение

Задача обеспечения информационной безопасности в Intranet оказывается более простой, чем в случае произвольных распределенных систем, построенных в архитектуре клиент/сервер. Причина тому - однородность и простота архитектуры Intranet. Если разработчики прикладных систем сумеют в полной мере воспользоваться этим преимуществом, то на программно-техническом уровне им будет достаточно нескольких недорогих и простых в освоении продуктов. Правда, к этому необходимо присовокупить продуманную политику безопасности и целостный набор мер процедурного уровня.

КАК ЗАЩИТИТЬ ИНФОРМАЦИЮ

Обеспечение безопасности при работе с компьютерной системой - задача многогранная. В ней можно выделить два основных направления: безопасность персонала и информационную безопасность. Оба аспекта составляют предмет жарких дискуссий ведущих специалистов отрасли на многочисленных совещаниях, семинарах и конференциях. Крупнейшим смотром технологий обеспечения информационной безопасности стала 23-я международная выставка-конференция, проводившаяся в Чикаго 12-13 ноября 1996 г., в которой участвовало более 100 компаний.

Остановимся подробнее на втором аспекте. Интерес к вопросам безопасности информации не случаен. Корпоративные системы электронного документооборота, бухгалтерского учета и управления базами данных получили широкое распространение в развитых странах уже в первой половине 70-х гг. С развитием компьютерных технологий, по мере снижения их стоимости, роста возможностей и доступности компьютеров, все больше компаний переходят на автоматизированные системы учета. В результате увеличиваются как объем информации, хранящейся на различных электронных носителях, так и ее ценность (которая, в первую очередь, определяется суммой возможных убытков при потере данных или их попадании к конкуренту). И тут-то выясняется, что электронные средства хранения даже более уязвимы, чем бумажные; размещаемые на них данные можно и уничтожить, и скопировать, и незаметно видоизменить. Последнее, кстати, представляет наибольшую опасность для компаний.

Что же означает потеря данных, на основе которых ведется управление бизнесом? По данным Миннесотского университета, 93% компаний, лишившихся доступа к своим данным на срок более 10 дней, покинули бизнес, причем половина из них заявила о своей

несостоятельности немедленно. Хотя компании, опасаясь за свое реноме, предпочитают замалчивать случаи крушения их информационных систем и вторжения в них, статистика подобных происшествий все же существует. Так, подкомитет по расследованиям при сенате США недавно провел соответствующий опрос среди 500 крупнейших индустриальных компаний страны. Более половины респондентов (264 фирмы) воздержались от ответа, однако 140 компаний признали, что их информационные системы подвергались нападениям в течение последнего года, и почти пятая часть из них сообщила, что понесенные при этом убытки составили свыше 1 млн дол.

В Российской Федерации такие исследования не проводились, но, конечно, события подобного рода иногда происходят. Например, в сеть одного крупного торгового зала проникли вирусы, и два дня, пока не была восстановлена информационная среда, фирма осуществляла только оптовые торговые операции. В результате оборот снизился в несколько раз, клиенты, не получавшие требуемых услуг, высказывали свое недовольство, персонал работал неэффективно, а системные администраторы в авральном порядке с утра до ночи "чистили" систему и восстанавливали информацию на дисках. Учитывая статистику Миннесотского университета, можно сказать, что фирма легко отделалась.

Российские предприниматели под давлением фактов, а иногда и личного опыта, наконец начали осознавать ценность информации, содержащейся в их корпоративных сетях. Следствием этого стало проявление некоторого, пока еще не слишком активного, интереса к системам безопасности. Немалую роль в продвижении технологий безопасности играют и отечественные системные интеграторы, в задачи которых входит создание комплексных информационных систем поддержки бизнеса и разработка технических и организационно-режимных мероприятий для повышения их безопасности. Государство, требующее от определенных организаций ответственного подхода к хранению и передаче информации, также стимулирует развитие данной области. В частности, Президент РФ своим указом от 3 апреля 1995 г. предложил Центральному банку (ЦБ) принять меры по отношению к коммерческим банкам, уклоняющимся от обязательного использования "защищенных технических средств хранения, обработки и передачи информации при их информационном взаимодействии с подразделениями ЦБ".

Правда, на сегодняшний день российские бизнесмены все же больше озабочены надежностью функционирования своих компьютерных систем и их защиты от вирусов, нежели созданием барьеров, ограждающих от несанкционированного доступа. Возможно, это пока оправданно, поскольку лишь немногие фирмы содержат в компьютерных сетях информацию, ценность которой адекватна расходам на ее извлечение.

Обсуждая вопросы безопасности информации в компьютерной системе со специалистами известных российских фирм, занимающихся системной интеграцией - таких как IBS, "ЛВС", "АйТи", "Анкей", "Оптима" и RPI, - авторы выделили два основных принципа организации информационных систем. Во-первых, это комплексный подход к построению системы, охватывающий как применение специальных аппаратных и программных средств, так и проведение организационно-режимных мероприятий. Во-вторых, высокие требования к квалификации обслуживающего персонала. Глобальными факторами, влияющими на функционирование системы и сохранность данных, являются сбой системы, случайное уничтожение ее отдельных компонентов и несанкционированный доступ к системе. Поскольку первые два фактора не связаны с прямой атакой на содержимое информационной системы, их можно объединить термином "несчастный случай".

Несчастный случай

К "несчастным случаям" мы относим неисправности оборудования, сбои в работе программного обеспечения (ПО), ошибки обслуживающего персонала, а также внешние воздействия - природные (землетрясения, ураганы, наводнения и т.п.), техногенные (пожары, перебои с энергоснабжением, прорывы водопровода и канализации и т. п.) и социальные (террористические акты, беспорядки, военные действия и т.д.). Российская

действительность такова, что отечественные компании подвержены воздействию всех этих факторов (возможно, не считая природных катаклизмов) в значительно большей степени, чем фирмы из экономически развитых стран.

На надежности систем отрицательно сказываются и наличие большого количества устройств, собранных из комплектующих низкого качества, и нередкое использование нелицензионного ПО. Аппаратное и программное обеспечение зачастую не отвечает требованиям совместимости, а "прописанная" в соответствующих файлах конфигурация систем - имеющимся аппаратным ресурсам. Виной тому может стать недостаточная компьютерная грамотность ответственных за поддержание компьютерной системы сотрудников. Иными словами, чрезмерная экономия средств (на обучение персонала, закупку лицензионного ПО и качественного оборудования) приводит к уменьшению времени безотказной работы и значительным затратам на последующее восстановление системы. Скупой, как известно, платит дважды.

Важным фактором является недостаточно высокая квалификация персонала. Авторы отнюдь не собираются оспаривать утверждение, что в России работает множество талантливых специалистов-компьютерщиков. Вопрос заключается в том, насколько эти таланты пригодны для выполнения обязанностей системного администратора корпоративной сети, в которой работают обычные бизнес-приложения. К сожалению, человек, обладающий мастерством на уровне хакерства и умеющий работать с разнообразным ПО и отлично разбираться в сложных ситуациях (что, безусловно, очень полезно), способен превратить информационную систему в цирк, на арене которого безостановочно сменяют друг друга версии и названия программ. Причем, как правило, замены производятся без глубокого понимания преимуществ нового пакета и не сопровождаются соответствующими организационными мероприятиями. Это и порождает различные сложные ситуации, которые затем мастерски преодолеваются (увы, не всегда быстро и без потерь). Должности системного администратора в большей степени соответствует другой тип специалиста - эмоционально устойчивый консерватор, способный реализовать комплексный подход для предупреждения внештатной ситуации, и руководствующийся в своей деятельности принципом Оккама "Не плоди сущности без надобности".

Что же касается внешних воздействий на информационную систему, то, действительно, ураганы и цунами в Москве - большая редкость, а землетрясения происходят в основном при появлении на улицах города большого числа бронетехники, но это уже другой фактор риска. Зато качество работы наших городских электросетей давно стало притчей во языцех, прорыв же канализации - и вовсе событие, значительно более вероятное, чем извержение вулкана или падение метеорита. Это усугубляет рискованность бизнеса, поскольку подобные несчастья, как правило, не относятся к разряду форс-мажорных обстоятельств, а, соответственно, компания не освобождается от штрафов в случае невыполнения обязательств.

В комплекс мероприятий по защите информационной системы от несчастных случаев специалисты компаний, занимающихся системной интеграцией, включают целый ряд действий, направленных на предотвращение внештатной ситуации, а не ликвидацию ее последствий. Разберем, для начала, средства, обеспечивающие бессбойную работу системы.

Источники бесперебойного питания

Компьютерная система энергоемка, и потому первое условие ее функционирования - бесперебойная подача электроэнергии. Необходимой частью информационной системы становятся источники бесперебойного питания для серверов, а по возможности, и для всех локальных рабочих станций. Специалисты компании IBS также рекомендуют дублировать электропитание, используя для этого различные городские подстанции. Такое решение особенно полезно для крупной корпоративной информационной системы, размещенной в большом городе, где перебои энергоснабжения чаще всего локализуются в одном

сегменте. В небольших городах, в которых электроснабжение значительно хуже, сотрудники фирмы "Оптима" советуют для кардинального решения проблемы устанавливать резервную силовую линию от собственного мотор-генератора (разумеется, с соблюдением всех норм пожарной безопасности).

Выбор надежного оборудования

Важнейшим фактором обеспечения надежности работы системы является подбор соответствующего оборудования. Практически все отечественные системные интеграторы рекомендуют заказчикам применять технику известных компаний, так называемый brand name. Такое оборудование проходит серьезный выходной контроль изготовителя, имеет высокий уровень совместимости и длительный срок гарантийного обслуживания.

Для гарантийного ремонта установленной техники в России существуют сервисные центры большинства компаний-производителей, созданные на базе либо представительства поставщика, либо отечественной компании, которая имеет необходимых специалистов и авторизована для выполнения такого рода работ. Поэтому, как правило, обещанный рекламой мировой уровень обслуживания становится доступным и российскому потребителю. Есть, конечно, и печальные исключения - скажем, Compaq и American Power Conversion (APC) уже стали классическими примерами производителей, "забывших" за океаном свой знаменитый сервис. Стандартный гарантийный срок на серверы и компьютеры (за исключением моделей низкого уровня) составляет три года, на периферийное оборудование - один год. Ряд производителей предоставляет гарантию типа on-site (с выездом специалиста к заказчику), другие за подобные услуги требуют дополнительную плату.

Как известно, производительность и живучесть информационной системы во многом зависит от работоспособности серверов. Большинство современных серверов обладают набором специальных аппаратных и программных средств, позволяющих предсказывать возможный выход из строя процессоров и жестких дисков. Во время гарантийного периода при поступлении сигнала о грядущем сбое устройства пользователь может потребовать от поставщика бесплатной замены подозрительного компонента, не дожидаясь его фактического отказа. При необходимости обеспечения круглосуточной бесперебойной работы информационной системы используются специальные отказоустойчивые компьютеры, т. е. такие, выход из строя отдельного компонента которых не приводит к отказу машины. В России наиболее известна высоконадежная техника компаний Stratus и Tandem. Из-за своей высокой стоимости она не получила в нашей стране широкого распространения и используется лишь крупными компаниями, бизнес которых в значительной степени зависит от работы компьютерной системы. Например, техника Tandem установлена примерно в полуторе десятков компаний, в число которых входят телекоммуникационная компания "Спринт", аэропорт "Пулково" и ING Bank.

Остается упомянуть о мелочах - сетевых розетках, разъемах, кабелях и т.д. Они также должны быть надлежащего качества, потому что система не сможет реализовать весь свой потенциал, если в ней окажется даже одна некачественная розетка.

Выбор программного обеспечения

Набор оборудования, связанного коммуникационными линиями, превращается в информационную систему, лишь получив свое внутреннее содержимое - программное обеспечение (ПО) и данные. Сама архитектура современных сетевых операционных систем (ОС) в значительной степени защищает их от некорректного обращения, и потому лишь немногие действия прикладных программ или драйверов периферийных устройств способны привести к их краху. Большинство бизнес-приложений сертифицированы для работы с популярными ОС. Тем самым фирма-разработчик операционной среды гарантирует корректную инсталляцию и работу приложения в данной ОС.

Многообразие периферийных устройств усложняет организацию обращения к ним из ОС и прикладных программ. Поэтому системные интеграторы рекомендуют при

выборе операционной среды обращать особое внимание на ее оснащенность драйверами и утилитами, перекрестную сертификацию оборудования и ПО, а также избегать использования доморощенных приложений. Помимо потенциальной несовместимости, последние имеют еще один недостаток - отсутствие поддержки производителя.

Среди сетевых операционных систем, используемых в России, наиболее популярны Microsoft Windows NT и Novell NetWare, причем в оценках доли рынка каждой из них мнения интеграторов расходятся. До недавнего времени NetWare лидировала со значительным отрывом, чему способствовало большое число специалистов и компаний, сертифицированных Novell. Сейчас этот разрыв достаточно быстро сокращается, растет число компаний со статусом Microsoft Solution Provider. Увеличение интереса к продуктам Microsoft во многом вызвано политикой компании, разумно вкладывающей значительные средства в обучение партнеров, в частности спонсирующей сдачу экзаменов системными инженерами Novell по курсам Microsoft. Что же касается Unix-систем, они поддерживаются ограниченным числом интеграторов и, видимо, большей частью ориентированы на российские отделения зарубежных компаний, исторически приверженных операционной системе UNIX.

Восстановление бизнеса после бедствия

Выбор надежного оборудования и ПО позволяет до определенной степени предотвратить сбой информационной системы. Однако встречаются и неподвластные системному администратору ситуации, влекущие за собой уничтожение информационной системы или какой-либо ее части. В условиях сложных деловых связей "падение" одной компании, к сожалению, ставит под удар функционирование многих ее партнеров. Некоторые из подобных ситуаций могут быть отнесены к разряду форс-мажорных, и потому связанное с ними невыполнение обязательств перед партнерами не повлечет за собой штрафных санкций. Некоторые, но далеко не все. Поэтому задача руководства компании - заранее определить ряд мероприятий, составляющих план восстановления бизнеса после бедствия (или Business Disaster Recovery, BDR), которые позволяют свести к минимуму потери информации и время простоя системы.

На Западе наличие такого плана стало обязательным для банков; изготовители оборудования требуют его от своих поставщиков. Достаточно заглянуть в хронику происшествий газет "Коммерсант" или "МК", чтобы понять, что многим компаниям на собственном опыте пришлось осознать необходимость подобного плана. В качестве примера можно вспомнить пожар в доме 4/17 по Покровскому бульвару, от которого пострадали офисы Hewlett-Packard, Московского народного банка, Union Bank of Switzerland и др.

По существу, восстановление бизнеса после бедствий представляет собой форму страховки, и потому возможно тесное взаимодействие фирм, предоставляющих услуги в этой области, со страховыми компаниями и фискальными структурами. Основу мероприятий, повышающих стойкость системы к подобного рода несчастьям, составляют различные формы резервирования и мультиплексирования оборудования и коммуникаций, принадлежащих к информационной системе.

Резервное копирование

Одним из ключевых моментов, обеспечивающих восстановление системы при аварии, является резервное копирование рабочих программ и данных. Несмотря на очевидность этой процедуры и ее относительную несложность, в некоторых организациях она производится недостаточно часто или игнорируется вообще. Опыт показывает: если содержимое системы копируется еженедельно в пятницу вечером, то все неприятности случаются в пятницу же, но в районе обеда. Резервное копирование должно сопровождаться целым рядом не менее очевидных организационных мероприятий. Носители - ленты или магнито-оптические диски - должны храниться за пределами серверной комнаты. Поскольку носитель используется многократно, нужно знать стандарты на число допустимых перезаписей и тесты, позволяющие определить степень

его изношенности. Широкий выбор устройств для копирования также может сыграть злую шутку с пользователями: о совместимости этих устройств следует позаботиться до того, как одно из них выйдет из строя.

Резервирование каналов связи

Лишенный связи с внешним миром и своими подразделениями, офис оказывается парализованным, и потому большое значение имеет резервирование внешних и внутренних каналов связи. Рекомендуется сочетать разные виды связи - кабельные линии и радиоканалы, воздушную и подземную прокладку коммуникаций и т.д.

По мере того как компании все больше и больше обращаются к Internet, их бизнес оказывается в серьезной зависимости от функционирования Internet-провайдера. У поставщиков доступа к Сети иногда случаются достаточно серьезные аварии. Скажем, в США в июне 1996 г. 12 часов не работала служба Netcom Online Communications Services, в августе на 19 часов отключилась America Online, в октябре встал на сутки один из почтовых серверов BBN, а в ноябре четверо суток не получали электронную почту пользователи WorldNet. В конце 1995 г. произошло вторжение в офис локального провайдера Internet в Атланте: бандиты "содрали" с компьютеров микросхемы памяти. Очевидно, что ущерб был причинен не только ограбленной компании. Сведения об авариях у отечественных провайдеров отсутствуют, однако они, скорее всего, не менее уязвимы, чем американские.

Какие меры может предпринять пользователь? Хранить все важные приложения во внутренней сети компании, поддерживать отношения с несколькими местными провайдерами, заранее изыскать путь оповещения стратегических клиентов об изменении электронного адреса и требовать от провайдера проведения мероприятий, обеспечивающих его оперативное восстановление после несчастного случая.

Дублирование, мультиплексирование и резервные офисы

Помимо резервного копирования, которое производится при возникновении внештатной ситуации либо по заранее составленному расписанию, для большей сохранности данных на жестких дисках применяют специальные технологии - "зеркалирование" дисков (запись осуществляется параллельно на два диска) и создание RAID-массивов. Последние представляют собой объединение нескольких жестких дисков. При записи информация поровну распределяется между ними - кроме одного, на который записываются так называемые "контрольные суммы". При выходе из строя одного из дисков находящиеся на нем данные могут быть восстановлены по содержимому остальных.

Симметричные многопроцессорные модели серверов, получающие все большее распространение, позволяют не только увеличить производительность машины за счет разделения задачи между несколькими процессорами, но и обеспечить ее самовосстановление при выходе из строя одного из процессоров. Hewlett-Packard производит машины, имеющие до 12 процессоров, DEC - до 14. Представители компании "ЛВС" называют фирму Sequent лидером в этой области: число процессоров в некоторых ее серверах достигает 30.

Технология кластеризации предполагает, что несколько компьютеров функционируют как единое целое. Кластеризуют, как правило, серверы. Один из серверов кластера может функционировать в режиме "горячего" резерва (не совершая транзакций), в полной готовности перенять эстафету от основной машины в случае ее выхода из строя. Возможна и параллельная обработка информации несколькими серверами. Кластерные технологии дороги, и потому наибольшее распространение в настоящее время получили кластеры из двух машин. Продолжением технологии кластеризации стала географическая, или распределенная, кластеризация, при которой через глобальную сеть объединяются несколько кластерных серверов, разнесенных на большое расстояние. Конечно, процесс обработки в данном случае не распараллеливается, однако на каждом сервере распределенного кластера отображаются все изменения базы данных.

Распределенные кластеры примыкают к понятию резервных офисов, ориентированных на обеспечение жизнедеятельности предприятия при уничтожении его центрального помещения. Условно их можно разделить на "холодные" (в которых проведена коммуникационная разводка, но отсутствует какое-либо оборудование) и "горячие" (ими могут быть дублирующий вычислительный центр, получающий всю информацию из центрального офиса, филиал, офис на колесах и др.).

Несанкционированный доступ к системе

Фирмы вынуждены защищать свои информационные системы не только от стихийных бедствий и сбоев аппаратуры, но и от доступа к ним посторонних лиц. Взаимоотношения систем защиты со средствами взлома подобны вечному соревнованию брони и снаряда: любая система безопасности, в принципе, может быть вскрыта. Эффективной можно считать такую защиту, стоимость взлома которой соизмерима с ценностью добываемой при этом информации. По степени сложности применяемых технических средств можно выделить три уровня несанкционированного доступа - низкий (вход в систему и получение в ней прав привилегированного пользователя), средний (прослушивание каналов передачи данных) и высокий (сканирование излучения).

Некоторую защиту от несанкционированного доступа предоставляют штатные средства прикладного и системного программного обеспечения. Для реализации более высокого уровня защиты необходимо использовать специальные средства шифрования и защиты информации. Особенностью рынка подобных средств является обязательная государственная лицензия на их создание, установку и эксплуатацию. Несмотря на многочисленные критические замечания в адрес государственного контроля над информационными системами независимых компаний, подобная практика находится в полном соответствии с действующим законодательством: правоохранительные органы по решению суда имеют право доступа к любым данным, содержащимся в информационных системах. Для того чтобы реально обеспечить подобный доступ, государство вынуждено ограничивать распространение систем защиты и иметь в своем распоряжении ключи для дешифровки.

Разработка, производство, эксплуатация или реализация шифровальных средств, предоставление услуг в области криптографии запрещены компаниям, не имеющим лицензий Федерального агентства правительственной связи и информации (ФАПСИ). Выдача лицензий на создание средств защиты данных находится в ведении Государственной технической комиссии (ГТК) и ФАПСИ. Также не разрешается ввозить в Россию без соответствующей лицензии криптографические средства иностранного производства. Таким образом государство ограничивает доступ зарубежных компаний на рынок средств обеспечения безопасности информации, который становится широким полем деятельности для российских разработчиков.

Защита от злоумышленника

Западная статистика показывает, что, как правило, проникновению злоумышленника в информационную систему компании способствуют либо некорректные действия администратора сети, либо умышленная или неумышленная помощь со стороны сотрудников. Причем в качестве предателя интересов компании в подавляющем большинстве случаев выступает ни кто иной, как представитель высшего эшелона власти. Последнее вполне объяснимо: топ-менеджер имеет широкий доступ к информации, понимает ее ценность и обладает достаточным кругом общения, для того чтобы ее продать. Подтверждается старинная русская пословица "От своего вора не убережешься". Противодействовать утечке информации через такие каналы позволяют, в первую очередь, организационно-режимные мероприятия (в том числе ограничение доступа к информации), о которых будет сказано ниже.

Что же касается устойчивости к нападениям извне, то, согласно "Оранжевой книге" Министерства обороны США, программное обеспечение может относиться к одному из следующих классов:

класс D - защита отсутствует, пользователь имеет неограниченный доступ ко всем ресурсам. К этому классу относятся операционные системы типа MS-DOS; класс C, наиболее популярный подкласс - C2. Доступ с паролем и именем. При работе с базой данных класса C пользователь, получив доступ к той или иной таблице базы, получает и доступ ко всем имеющимся в ней данным. К этому классу относится большинство сетевых операционных систем; класс B, наиболее употребительный подкласс - B1. Базы данных класса B позволяют дифференцировать доступ к данным для разных пользователей даже внутри одной таблицы. Улучшенные с точки зрения безопасности реализации стандартных операционных систем производят многие фирмы (DEC, Hewlett-Packard, Santa Cruz Operations, Sun); класс A - наиболее защищенные операционные системы, которые российские системные интеграторы рекомендуют использовать только при построении сетевой защиты от внешнего мира (создании брандмауэра).

Надо заметить, что вероятность несанкционированного входа в систему возрастает при ее перегрузках, которые возникают, например, при массовом подключении к ней пользователей (в начале рабочего дня). Хакеры иногда создают сходную ситуацию, направляя в систему поток сообщений, которые она не в состоянии корректно обработать. В результате создается открытый канал, через который возможен несанкционированный доступ. Таким образом, наличие брандмауэра как средства, предоставляющего более высокую степень защиты, оказывается вполне оправданным. На фоне массового подключения к Internet брандмауэры начали устанавливать и российские компании. По оценкам специалистов компании "ЛВС", в России пользуются спросом сравнительно недорогие машины (стоимостью около 5 тыс. дол.) с операционной системой UNIX, сертифицированной по классу C2.

СУБД также предоставляют определенный уровень защиты, позволяя разграничить доступ к данным для разных категорий пользователей. Во-первых, информацию, доступную разным классам пользователей, можно хранить в разных таблицах. Во-вторых, содержащуюся в таблице информацию пользователь может получать через некоторое промежуточное представление, или вид, охватывающий лишь определенную часть таблицы (скажем, три колонки из пяти). В-третьих, можно ограничить права на выполнение отдельных модулей, время использования центрального процессора, число физических считываний с диска за определенный промежуток времени. Таким образом, возможны ситуации, когда любой запрос пользователя обрабатывается, но очень медленно.

Серверы обладают различными встроенными средствами защиты - защитой от выключения питания; двухуровневой системой паролей (для пользователя и системного администратора), реализованной средствами BIOS; паролями на съемные компоненты (диски); блокировкой клавиатуры; гашением монитора.

Однако сами по себе оборудование и ПО не в состоянии обеспечить защиту данных. Система безопасности должна быть грамотно настроена, что обуславливает особые требования к квалификации системного администратора. Конфигурирование операционной системы класса C2 представляет собой сложную задачу. Кроме того, технические меры необходимо дополнять рядом организационно-режимных мероприятий: ограничением доступа на предприятие и в различные его подразделения; выделением специальных устройств для работы с секретной информацией (человек, имеющий доступ к закрытой информации, не сможет выводить свои данные на сетевой принтер); регулярной сменой паролей и наложением административных санкций за их разглашение или уход с рабочего места без выхода из системы; запретом на использование в качестве паролей имен, фамилий и других легко угадываемых слов.

Большое значение для безопасности информационной системы имеют такие акции системного администратора, как своевременное обновление программного обеспечения. Как правило, при выходе новой версии немедленно становится общедоступной информация об ошибках предыдущей (в том числе о недостатках системы защиты). Если

обновление не было вовремя произведено, вероятность взлома системы многократно возрастает. Впрочем, иногда возникают и противоположные ситуации. В качестве примера можно упомянуть операционную систему Microsoft Windows NT 3.5, которая сертифицирована по стандарту безопасности C2. Однако следующая версия, Windows NT 3.51, ни по какому стандарту безопасности не сертифицирована. Следовательно, системный администратор, сменивший 3.5 на старшую 3.51, взял на себя ответственность за безопасность бизнеса фирмы. Только сообщить об этом руководству он, скорее всего, забыл.

При соблюдении всех правил конфигурирования программного обеспечения и проведения административных мероприятий вероятность несанкционированного доступа к информации значительно снижается. Штатные возможности программного обеспечения могут быть дополнены рядом технических средств (смарт-картами, магнитными ключами, использованием интеллектуального оборудования, например концентраторов с защитой на порт, структуризацией локальной сети с ограничением прав доступа к ее отдельным сегментам) и специальными программами мониторинга и защиты сетей. В частности, фирма "АйТи" рекомендует своим клиентам программу SecretNet производства российской компании "ИнформЗащита".

Защита данных от перехвата

С помощью вышеперечисленных способов защиты можно предотвратить несанкционированное обращение к приложению или базе данных. Но информация, как известно, передается по сети; прослушивая канал связи, ее удается перехватить. ФАПСИ разделяет коммуникации на три класса. Первый охватывает локальные сети, расположенные в так называемой "зоне безопасности" (территории с ограниченным доступом и заэкранированным электронным оборудованием и коммуникационными линиями) и не имеющие выходов в каналы связи за ее пределами. Ко второму классу относятся каналы связи вне "зоны безопасности", защищенные организационно-техническими мерами (например, оптоволоконный кабель), а к третьему - незащищенные каналы связи общего пользования. Применение коммуникаций второго класса значительно снижает вероятность перехвата данных.

Для защиты информации во внешнем канале связи используются следующие устройства: скремблеры (при защите речевой информации, передаваемой по обычным телефонным каналам связи в режиме точка-точка), шифраторы/дешифраторы (для широковещательной связи) и криптографические средства, обеспечивающие шифрование передаваемого пакета. Однако их применение сопряжено с получением лицензий, что не всегда удается организовать оперативно. Поэтому интеграторы используют открытые для свободной эксплуатации средства, затрудняющие интерпретацию перехваченного пакета. Например, компания "ЛВС" предлагает туннелировать данные из одного сетевого протокола в другой.

Столь изощренные способы проникновения в информационную систему, как контроль излучения монитора, в России маловероятны, поскольку требуют оснащения на уровне технической разведки. Вероятно, российские корпоративные сети еще не хранят столь ценную информацию, чтобы заинтересовать подобные структуры.

Защита информационной системы представляет собой комплекс дорогих технических средств и организационных мероприятий. По оценкам фирмы "АйТи", некоторые банки тратят на обеспечение сохранности информации до 30% стоимости всей компьютерной системы. В эту сумму не входят расходы на повышение квалификации системного администратора или менеджера по безопасности, во многом и определяющей надежность системы защиты. Разнообразные учебные центры предлагают достаточно длинный список курсов по администрированию тех или иных средств. Авторы затрудняются выделить среди них учебный цикл, в котором акцент делается на выбор, конфигурирование и управление средствами безопасности. Тем большее значение имеет

взаимодействие заказчика с системным интегратором с целью обучения и последующего консультирования его персонала.

ЧЕЛОВЕЧЕСКИЙ ФАКТОР И БЕЗОПАСНОСТЬ

Техническое развитие человечества сопровождается передачей человеку все большего числа управляющих функций, позволяя ему все больше отдаляться от орудий труда и превращаться из исполняющего в управляющий орган системы производства. Такая трансформация роли человека приводит к замене физического труда умственным, снижая необходимость мышечной работы и соответствующих энергозатрат. Однако при этом значительно возрастает нагрузка на психику человека, которому приходится решать задачи оценки и прогнозирования эффективности работы оборудования и других людей, надежного взаимодействия с различными элементами социотехнической системы производственного механизма. Согласно статистике, более половины аварий в социотехнических системах (в авиации до 90% происшествий) связаны с человеческим фактором из-за возрастания концентрации управляемой мощности в руках одного человека.

n грамотное обеспечение эргономических требований увеличивает производительность на 100%.

n хорошее освещение рабочего места увеличивает производительность труда на 20%.

n снижение шума до гигиенических норм повышает производительность труда на 40-50%, а продуманное введение музыки на 12-14%.

n оптимальная окраска помещений и оборудования повышает производительность на 25% и снижает непроизводительные потери рабочего времени на 32%.

Аварии приводят к значительным человеческим и экономическим потерям. Однако не только такие "фатально-летальные" события сопровождают технический прогресс информационного общества. "Тихие" события, происходящие в банках, управленческих офисах, могут приводить к катастрофам и глобального масштаба, так как информационное пространство уже не локализовано в одном помещении, одном учреждении и даже одной стране. "Утечка" конфиденциальной информации о деятельности предприятия (целенаправленная или непроизвольная) либо уход ведущих специалистов могут небольшую компанию привести к гибели.

Универсальные черты корпоративной культуры безопасности

n личное осознание важности безопасности;

n знания и компетентность, обеспечиваемые подготовкой и инструкциями для персонала, а также его самоподготовкой;

n приверженность приоритетам безопасности, демонстрируемая на уровне старших руководителей; понимание общих целей безопасности каждым из работников;

n усиление мотивации путем использования административных методов (постановка целей, создание системы поощрений и наказаний, а также формирование у персонала личной позиции по отношению к безопасности корпорации);

n надзор (практика ревизий и экспертиз);

n готовность реагировать на критику, независимо от иерархического уровня;

n ответственность персонала, вырабатываемая через формальное установление и описание должностных обязанностей и понимание их работниками.

Безопасность персонала

Безопасность отдельного человека и коллектива становится функцией психофизиологического соответствия человека требованиям профессии. На бытовом уровне работа специалиста управленческой сферы кажется легкой и общедоступной. Все понимают, что носить пятипудовые мешки по силам далеко не каждому. К сожалению, не всем известно, что работать с интенсивными потоками информации также могут не все люди, а во многих случаях попытка справиться с такой "легкой" задачей приводит к невротизации личности и к таким заболеваниям, как гипертония, язва желудка и

двенадцатиперстной кишки, инфаркты, инсульты и т.п. Прогнозирование потенциального нарушения здоровья и безопасности человека позволяет избежать ненужных потерь времени и средств на освоение профессии и поддержание ее на необходимом уровне.

Опыт использования системы показал, что негативное (настороженное) на первых порах отношение пользователей через некоторое время сменилось не только доверием к результатам тестирования, но и потребностью в ежедневном использовании системы. Правда, по имеющимся данным наблюдения за группой из 89 пользователей, интерес к использованию системы оказался прямо пропорционален стремлению к достижению высоких профессиональных результатов. Так, на одном из первых предприятий, начавших работать с системой, 15 из 36 человек продолжали работать через год, причем пять из них вскоре перешли на более высокие должности. На трех других предприятиях активно начали пользоваться ежедневным тестированием около 20% персонала, причем, по оценкам экспертов, практически все они относились к группе наиболее квалифицированных сотрудников.

Вопросами профессионального отбора людей для выполнения определенных социотехнических задач человечество начало уделять внимание еще 2 тыс. лет тому назад. К настоящему времени систему индивидуального психофизиологического мониторинга умственной работоспособности человека, разработанную первоначально для операторов предприятий энергетики и авиакосмической отрасли, используют более 200 зарегистрированных пользователей.

Человеческий фактор

В повседневной жизни при всей индивидуальности восприятия наши оценки совпадают в большинстве случаев с такими же оценками других людей. Совершенно естественно, что такие обобщения требований к предметной среде и ее оптимизации со временем привели человечество к выработке неких обобщенных критериев и требований, ставших основой науки о труде эргономики ("эргос" труд, "номос" закон), более известной в предыдущие десятилетия в англоязычных странах как "человеческий фактор" (human factors).

В связи с изменением характера труда в XX веке и тенденцией перехода от физического к умственному труду сегодня эргономику (или человеческий фактор) можно определить как интерфейс человека с техническими средствами и окружающей средой, причем он имеет огромный потенциал для совершенствования здоровья, безопасности и комфорта как самого человека, так и систем производства. Это мнение одного из ведущих и общепризнанных авторитетов мировой эргономики Х. Хендрика (США) разделяет большинство других специалистов. Но почему в таком случае крупные организации, с их большой заинтересованностью в увеличении доходов, уменьшении расходов и росте производительности не ломятся к эргономистам за помощью или не создают условия для развития эргономики за пределами ее сегодняшних возможностей? Почему соответствующие ветви государственной власти не развивают законодательство, относящееся к человеческому фактору/эргономике? Почему и государственные мужи, и руководители предприятий на эргономику чаще смотрят как на дополнительный груз расходов и увеличение затрат производства? По мнению Х. Хендрика, существуют, по крайней мере, четыре причины такого положения дел.

Во-первых, некоторые из этих индивидуумов и организаций столкнулись с плохой эргономикой, или "эргономикой колдовства", как в форме продуктов, так и рабочих сред, долженствующих быть разработанными именно в эргономическом плане, однако этого не произошло; иные же эргономические разработки просто были выполнены некомпетентными лицами.

Другая хорошо известная нам причина состоит в том, что "каждый сам себе голова". Каждый "управляет" системами ежедневно (автомобилем, компьютером, ТВ, социумом). Это порождает иллюзию знания человеческого фактора, хотя в действительности является не более чем обывательским "здравым смыслом". Даже опытные эргономисты имеют

собственный список так называемых решений "здравого смысла", которые закончились серьезными происшествиями, авариями или экономическим ущербом, как результат несоответствия такого "здравого смысла" реалиям жизни.

В-третьих, мы иногда полагаем, что менеджеры активно поддержат эргономику просто потому, что "это правильно". На самом же деле, западным менеджерам (у нас, к сожалению, даже до этого пока не дошло) необходимо как бы резервировать возможность "оправдания своего вклада" в обеспечение конкурентоспособности и выживаемости организации либо использовать эргономику в качестве "эвристического поиска какого-нибудь выхода из сложной ситуации". Но эргономика не является панацеей от всех бед и достаточным основанием для "массированных" нововведений. Любое решение должно основываться на реальной оценке ситуации

Способы принятия решений

Рутинный

Руководитель ведет себя в соответствии с имеющейся программой. Его задача распознавание ситуации и разрешение ее по готовой программе. Такие ситуации должны быть предсказуемыми. Функция руководителя заключается в том, чтобы "почувствовать", идентифицировать ситуацию, а затем взять на себя ответственность за начало определенных действий.

Для успешного решения проблем руководитель должен обладать не только способностью "чувствовать" ситуацию, но и уметь трактовать имеющуюся программу действий в соответствии со сложившимися условиями, проявлять решительность в обеспечении эффективных действий в нужное время, действовать логично. На этом уровне не требуется творческого подхода, поскольку все процедуры заранее предписаны.

Селективный

Для этого уровня необходимы инициатива и свобода действий, однако в определенных границах. Здесь руководитель оценивает достоинства целого круга возможых решений и старается выбрать из некоторого числа хорошо отработанных альтернативных наборов действий те, которые лучше всего подходят к данной проблеме. Для такого рода решений необходимо обладать умением выбирать направление действий с максимальной вероятностью их приемлемости, экономичности и эффективности.

Адаптационный

На этом уровне встречаются дополнительные трудности, поскольку необходимо найти творческое решение, которое (в определенном смысле) может быть абсолютно новым.

Обычно здесь имеются наборы проверенных возможностей и некоторые новые идеи. Успех руководителя в решении этого типа проблем будет зависеть от его личной инициативности и способности сделать "прорыв в неизвестное". Подобные решения дают ответ на проблемы, которые могли существовать и ранее, но в иной конкретной форме. Иначе говоря, руководитель ищет новое решение известной проблемы.

Инновационный

Проблемы этого типа наиболее сложны, ведь они требуют особых способностей. Для их решения нужен принципиально новый подход. Зачастую такой проблемой может быть та, которую плохо поняли ранее, и для ее решения необходимы абсолютно новые представления и методы. Могут возникать и другие препятствия, преодоление которых потребует создания новой отрасли науки.

ЛИТЕРАТУРА

1. Медведовский И.Д., Семьянов П.В., Леонов Д.Г. «Атака на интернет»

2. Издательского дома "Открытые Системы" (Lan Magazine/Журнал сетевых решений, 1996, том 2, #7)

3. Издательского дома "Открытые Системы"(Сети, 1997, #8)

4. “Office” N5 1999 Александр Буров «Человеческий фактор и безопасность»

Перечень тем индивидуальных домашних заданий (рефератов)

1. Краткий исторический обзор развития теории электромагнетизма от средних веков до наших дней.
2. Ученые и изобретатели, с чьими именами связана история и нынешние успехи радиотехники.
3. Элементная база радиотехники и ее эволюция.
4. Диапазоны радиоволн и области их применения при построении различных радиотехнических систем.
5. Радиоэлектроника в социально-экономической и культурной жизни общества.
6. Радиоэлектроника в быту.
7. Радиотехнические устройства пожарной и охранной сигнализации
8. Основные принципы и история развития радиолокации и радионавигации.
9. Основные принципы и история развития телевизионной техники.
10. Радиоэлектроника в банковском деле.
11. Радиоэлектроника в медицине.
12. Радиоэлектроника в системах экологического мониторинга.
13. Роль радиотехники в освоении человеком космического пространства.
14. Этапы развития радиотехники и электроники.
15. Правовые основы защиты информации.
16. От "грозоотметчика" А. С. Попова до цифрового радиоприемника. Развитие теории и техники радиоприемных устройств.
17. От искрового передатчика до оптического квантового генератора. Развитие теории и техники радиопередающих устройств.
18. От транзистора до большой интегральной схемы. Развитие полупроводниковой техники и технологии.
19. От «Эниак-2» до суперкомпьютера. Развитие цифровой электронно-вычислительной техники.
20. От «шифра Цезаря» до цифровой подписи. Развитие теории и техники криптографии.
21. Понятие и основные свойства информации как объекта защиты.
22. Современные системы радиосвязи.
23. Системы сотовой связи. Методы обработки сигналов и методы защиты.
24. Радиосистемы персонального вызова. Пейджинговая связь.

25. Современные телевизионные системы. Принципы передачи и приема телевизионных сигналов. Телевизионные стандарты.

26. Устройства сопряжения компьютера и канала связи. Их назначение и характеристика.

27. Архитектура компьютерных сетей. Виды, назначение и характеристика протоколов межуровнего обмена информацией.

28. Взаимообусловленность прогресса информационных технологий и проблем обеспечения информационной безопасности.

29. Человеческий фактор в реализации угроз и обеспечения безопасности информацией, обрабатываемой в компьютерных системах.

30. Общая характеристика технических каналов утечки информации.

31. Системы радиотехнической разведки.

32. Понятие несанкционированного доступа к информации, формы, способы, средства его реализации.

33. Компьютерные вирусы: классификация, результаты воздействия.

34. Реализация несанкционированного доступа на основе использования программных закладок.

35. Криптографические методы защиты информации.

Объем реферата составляет от 10 до 15 страниц. Текст реферата печатается на листах формата А4. Поля на листах: слева – 30 мм, справа – 10 мм, сверху – 20 мм, снизу – 20 мм. Использовать шрифт Times New Roman кегль 14, интервал 1,5. Все страницы отчета нумеруются по порядку от титульного листа до последней страницы. Первой страницей считается титульный лист, на ней цифра 1 не ставится, на следующей странице ставится цифра 2 и т.д. Порядковый номер печатается справа внизу страницы. Разделы нумеруются согласно требований ГОСТ 1.5-68 арабскими цифрами и разделяются точками.

Заголовки разделов выполняются с выравниванием абзаца «по центру» (абзацный отступ 0 мм), начиная с нового листа. Расстояние от текста до следующего заголовка должно быть 12 пунктов, а от заголовка до следующего за ним текста - 6 пунктов. Таблицы, рисунки, формулы нумеруются последовательно арабскими цифрами в пределах раздела, если в отчете есть на них ссылки.

Текст отчета должен быть отредактирован и напечатан с соблюдением правил оформления научных работ, предусмотренных ГОСТом.